

Lösningar tenta TENB SF1630(/1631) DISKRET MATEMATIK, D3

13 mars 2014

Tryckfel kan förekomma.

- 1a) (1p) $(G, \circ)$ är en grupp omm 1. $(x \circ y) \circ z = x \circ (y \circ z)$ för alla $x, y, z \in G$ (associativitet),
 2. Det finns $e \in G$ sådant att $e \circ x = x \circ e = x$ för alla $x \in G$ (identitetsselement) och
 3. För varje $x \in G$ finns $x^{-1} \in G$ med $x \circ x^{-1} = x^{-1} \circ x = e$ (inverseelement).

(Villkoret om slutenhet behövs inte, eftersom vi förutsatt att $\circ : G \times G \rightarrow G$.)

- b) (1p) $Z(G) = \{z \in G \mid zg = gz \text{ för alla } g \in G\}$, de $z \in G$ som kommuterar med alla $g \in G$.

- c) (1p) En högersidoklass till H är en mängd av formen $Hg = \{hg \mid h \in H\}$ för något $g \in G$.

- 2a) (1p) Stabilisatorn för $x \in X$ är $G_x = \{g \in G \mid gx = x\}$ (gx är resultatet av g 's verkan på x).

- b) (1p) Antalet banor är $\frac{1}{|G|} \sum_{g \in G} |F(g)|$, där $F(g) = \{x \in X \mid gx = x\} (= X_g)$.

- c) (1p) $U(\mathbb{Z}_{20}) = \{x \in \mathbb{Z}_{20} \mid \text{sgd}(x, 20) = 1\} = \{1, 3, 7, 9, 11, 13, 17, 19\}$.

- 3a) (1p) För $k = 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19$ (för alla primtalspotenser).

- b) (1p) $(F \setminus \{0\}, \cdot)$ är en cyklisk grupp.

- c) (1p) $F[x]/(k(x))$ är en kropp omm $k(x)$ är irreducibelt (inte en produkt av faktorer av grad ≥ 1).

- 4a) (1p) $\delta = \min\{\partial(x, y) \mid x, y \in \mathcal{C}, x \neq y\}$, där $\partial(x, y) = |\{i \mid x_i \neq y_i\}|$.

- b) (1p) $x \in \mathbb{Z}_n$ krypteras som $E(x) = x^e \in \mathbb{Z}_n$.

- c) (1p) Nej, t.ex. är $2^{10} = 1024 = 3 \cdot 11 \cdot 31 + 1 \equiv_{11} 1$ och $\equiv_{31} 1$, så $2^{11 \cdot 31 - 1} \equiv_{11 \cdot 31} 1$ ($341 = 11 \cdot 31$ är ett pseudoprimtal med bas 2). Men "endast om" gäller.

- 5) (3p) Vi söker en delgrupp till S_4 som är isomorf med kvadratens symmetrigrupp $G_{\square}$.

Lösning:

Eftersom en rotation av kvadraten bestäms helt av motsvarande bijektion av hörnen, fås en isomorfi genom att låta element i $G_{\square}$ motsvara de permutationer av hörnen de ger.

Kalla hörnen, i ordning, 1, 2, 3 och 4. id ger då permutationen (1), (övriga) rotationer kring en axel vinkelrät mot kvadraten ger (1 2 3 4), (1 3)(2 4) och (1 4 3 2), rotationer kring axlar parallella med kvadratens kanter ger (1 2)(3 4), (1 4)(2 3) och de kring diagonalerna ger (1 3), (2 4). Att dessa element utgör en delgrupp till S_4 följer av att $G_{\square}$ är en grupp.

Svar: $G_{\square} \approx \{(1), (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3), (2\ 4)\}$.

- 6) (3p) Gruppen $G = U(\mathbb{Z}_{18})$ verkar på mängden $X = \mathbb{Z}_{18}$ med multiplikation. Vi söker alla banor.

Lösning:

Banorna är $Gx = \{gx \mid g \in G\}$ för olika $x \in X$.

G innehåller precis de $x \in \mathbb{Z}_{18}$ som har $\text{sgd}(x, 18) = 1$ (de inverterbara, enligt känd sats), dvs $G = \{1, 5, 7, 11, 13, 17\}$.

Man finner $G0 = \{0\}$, $G1 = \{1, 5, 7, 11, 13, 17\} = G$, $G2 = \{2, 10, 14, 4, 8, 16\}$, $G3 = \{3, 15, 3, 15, 3, 15\} = \{3, 15\}$. Eftersom $4 \in G2$ är $G4 = G2$ och p.s.s. är $G5 = G1 = G$, men $G6 = \{6, 12, 6, 12, 6, 12\} = \{6, 12\}$ och $G9 = \{9, 9, 9, 9, 9, 9\} = \{9\}$. Alla G 's element finns med i precis en av dessa, så det är alla banorna.

Svar: Banorna är $\{0\}, \{1, 5, 7, 11, 13, 17\}, \{2, 4, 8, 10, 14, 16\}, \{3, 15\}, \{6, 12\}, \{9\}$.

- 7) (3p) Vi söker $\text{sgd}(f(x), g(x))$ i $\mathbb{Z}_5[x]$, då $f(x) = x^4 + x^3 + 4x^2 + 3x + 4$, $g(x) = x^4 + x^2 + 3x + 1$.

Lösning:

Euklides algoritm. Man finner att $f(x) = 1 \cdot g(x) + (x^3 + 3x^2 + 3) = f(x) + h(x)$ och med polynomdivision $g(x) = (x + 2)h(x)$. Det betyder att $\text{sgd}(f(x), g(x)) = h(x) = x^3 + 3x^2 + 3$.

Svar: $\text{sgd}(f(x), g(x)) = x^3 + 3x^2 + 3$.

8) Vi har en linjär, binär kod med kontrollmatrisen $H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}$ och de mottagna orden 11001, 01010, 10101. Vi söker de sända kodorden, då högst ett fel har uppstått i varje.

Lösning:

Matrismultiplikation ger $H(11001)^T = (000)^T$. $H(01010)^T = (100)^T$, H :s tredje kolonn. $H(10101)^T = (010)^T$, H :s fjärde kolonn. Det har alltså blivit fel i ingen, tredje respektive fjärde positionen.

Svar: De sända kodorden var 11001, 01110 respektive 10111.

9) (4p) G är en grupp och $A \subseteq G$, $A \neq \emptyset$.

Vi skall visa att om $G_A = \{g \in G \mid ga \in A \text{ för alla } a \in A\}$ måste $|G_A| \leq |A|$.

Lösning:

Beviset grundar sig på att $g \in G_A$ bestäms helt av sin verkan på ett enda a .

Tag ett $a \in A$ (finns, ty $A \neq \emptyset$). Om $g_1, g_2 \in G_A$ och $g_1a = g_2a$ är $g_1 = g_2$ (ty $a \in G$, multiplicera med a^{-1} från höger). Det betyder att $f_a : G_A \rightarrow A$ som ges av $f_a(g) = ga$ är en injektion, så $|G_A| \leq |A|$ (postfacksprincipen). **Saken är klar.**

10) Vi söker antalet väsentligt olika liksidiga trianglar (brickor) med en röd, gul eller blå kula i varje hörn och varje yta vit eller svart då (a, 3p) man bara kan vrida så att ytorna inte byter plats och (b, 1p) man också kan vrida så att ytorna byter plats.

Lösning:

Vi använder Burnsides lemma (Thm 21.4 i Biggs). (Det går också att räkna "för hand".)

Symmetrigruppen G_Δ har 6 element, av tre typer:

- identitets"rotationen", id ,
- 2 rotationer $\pm \frac{2\pi}{3}$ kring axeln genom triangelns tyngdpunkt, vinkelrät mot dess plan, rot_v ,
- 3 rotationer π kring triangelns höjder, rot_h .

$|F(g)|$, antalet konfigurationer som inte ändras av g , är $3^m \cdot 2^n$, där m är antalet banor för hörnen under $\langle g \rangle$:s verkan ($\langle g \rangle$ är den cykliska delgrupp till G som genereras av g) och n motsvarande för ytorna (alla i samma bana måste ha samma färg och banornas färger kan väljas på 3^m , 2^n sätt).

För de olika $g \in G$ blir det:

g	antal g	$ F(g) $
id	1	$3^3 \cdot 2^2$
rot_v	2	$3^1 \cdot 2^2$
rot_h	3	$3^2 \cdot 2^1$

Så antalet olika smyckade trianglar = antalet banor under G :s verkan på färgningarna =

a. (bara id och rot_v) = $\frac{1}{|G|} \sum_{g \in G} |F(g)| = \frac{1}{3} (3^3 \cdot 2^2 + 2 \cdot 3 \cdot 2^2) = 3^2 \cdot 2^2 + 2^3 = 44$.

b. (hela G_Δ) = $\frac{1}{|G|} \sum_{g \in G} |F(g)| = \frac{1}{6} (3^3 \cdot 2^2 + 2 \cdot 3 \cdot 2^2 + 3 \cdot 3^2 \cdot 2) = 3^2 \cdot 2 + 2^2 + 3^2 = 31$.

Svar a: 44 olika brickor, b: 31 olika brickor.

11) p och q är olika primtal. Vi söker alla $k \in \mathbb{N}$ sådana att $x^k \equiv_{p \cdot q} x$ för alla $x \in \mathbb{Z}$.

Lösning:

Eftersom p och q är relativt prima: $x^k \equiv_{p \cdot q} x \Leftrightarrow (x^k \equiv_p x \text{ och } x^k \equiv_q x)$ (entydig faktorisering i $\mathbb{Z}$ ger $p \cdot q \mid (x^k - x) \Leftrightarrow (p \mid (x^k - x) \text{ och } q \mid (x^k - x))$), så kongruensen gäller för alla $x \in \mathbb{Z}$ om $x^k = x$ för alla x i både $\mathbb{Z}_p$ och $\mathbb{Z}_q$. För x inverterbart i $\mathbb{Z}_p$ (dvs $x \neq 0$) är $x^k = x$ ekvivalent med $x^{k-1} = 1$, dvs $(p-1) \mid (k-1)$ (eftersom $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ är en cyklisk grupp av ordning $p-1$ finns ett element av ordning $p-1$ och allas ordningar är delare till det (känd följd av Lagranges sats). För $x = 0$ duger alla $k > 0$. Med motsvarande för q fås att de sökta k är precis de som uppfyller både $(p-1) \mid (k-1)$ och $(q-1) \mid (k-1)$, så alla $k = n \cdot \text{mgm}(p-1, q-1) + 1$, $n \in \mathbb{N}$.

Svar: Alla $k = n \cdot \text{mgm}(p-1, q-1) + 1$, $n \in \mathbb{N}$.

12) Vi söker (a, 1p) $|R|$ och (b, 4p) alla lösningar till ekvationen $t^2 + 7t + 9 = 0$ i ringen $R = \mathbb{Z}_{11}[x]/(x^2 + 1)$. Vi kallar restklassen som innehåller x för α .

Lösning:

a. Varje restklass i R innehåller precis ett polynom av grad ≤ 1 (och alla sådana ligger förstås i sin restklass), så elementen i R kan skrivas $a + b\alpha$, där olika $a, b \in \mathbb{Z}_{11}$ ger olika element. Det ger att $|R| = 11^2 = 121$.

b. $t^2 + 7t + 9 = t^2 + 18t + 9 = t^2 + 18t + 4 + 5 = (t + 9)^2 + 5$, så ekvationen kan skrivas $(t + 9)^2 + 5 = 0$. $t + 9$ måste alltså vara ett element i R med kvadraten $-5 = 6$. Kvadraterna av elementen i $\mathbb{Z}_{11} = \{0, 1, 2, 3, \dots, 10\}$ är $0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1$, alla skilda från 6, men eftersom $x^2 = (x^2 + 1) - 1$ är $\alpha^2 = -1$ och $(4\alpha)^2 = (7\alpha)^2 = 5(-1) = -5 = 6$, så $t + 9 = 4\alpha, 7\alpha$ ger lösningar till ekvationen: $t = -9 + 4\alpha, -9 + 7\alpha = 2 \pm 4\alpha$.

Det finns inget element i $\mathbb{Z}_{11}$ med kvadrat -1 , så $x^2 + 1$ är irreducibelt (andragradspolynom utan nollställe) och R alltså en kropp. Det följer att en andragradsekvation kan ha högst två nollställen i R och vi har funnit alla lösningar.

Svar a: $|R| = 121$, **b:** Alla lösningar är $t = 2 \pm 4\alpha$.

13) Vi söker (a, 1p) antalet inverterbara element i $\mathbb{Z}_{299}$ och (b, 4p) ett element av ordning 33 i gruppen $(U(\mathbb{Z}_{299}), \cdot)$. [$299 = 13 \cdot 23$]

Lösning:

a. Antalet inverterbara element är $\phi(299) = (13 - 1)(23 - 1) = 12 \cdot 22 = 264$.

b. $x^n \equiv_{299} 1$ omm både $x^n \equiv_{13} 1$ och $x^n \equiv_{23} 1$ [ty $299 \mid x^n - 1 \Leftrightarrow (13 \mid x^n - 1 \text{ och } 23 \mid x^n - 1)$], så om $a \in U_{13} (= (\mathbb{Z}_{13} \setminus \{0\}, \cdot))$ har ordning 3, $b \in U_{23}$ har ordning 11 och $x \equiv_{13} a, x \equiv_{23} b$, gäller $x^n = 1$ i U_{299} omm $3 \mid n$ och $11 \mid n$, dvs omm $33 \mid n$, så ett sådant x har ordning 33 i U_{299} . Sådana a, b finns, ty U_{13}, U_{23} är cykliska grupper (multiplikativa gruppen i kropparna (13 och 23 är ju primtal) $\mathbb{Z}_{13}$ resp. $\mathbb{Z}_{23}$) av ordning 12 resp. 22. Man finner i U_{13} : $2^2 = 4, 2^3 = 8, 2^4 = 3, 2^6 = 12$, så 2 genererar U_{13} (ordningen måste ju vara en delare till 12) och $2^4 = 3$ har ordning 3 i U_{13} . I U_{23} : $2^2 = 4, 2^{11} = 2048 = 1$, så 2 har ordning 11 i U_{23} .

Återstår att finna x med $x \equiv_{13} 3, x \equiv_{23} 2$.

$x \equiv_{13} 3$ omm $x = 3 + 13y$ för något $y \in \mathbb{Z}$. Då gäller $x = 3 + 13y \equiv_{23} 2$ omm $13y \equiv_{23} -1$ omm (eftersom $\text{sgd}(2, 23) = 1$) $3y \equiv_{23} 26y \equiv_{23} -2$ omm (eftersom $\text{sgd}(8, 23) = 1$) $y \equiv_{23} 24y \equiv_{23} -16 \equiv_{23} 7$, dvs $y = 7 + 23z$ för något $z \in \mathbb{Z}$. Så $x = 3 + 13(7 + 23z) = 94 + 299z$ och $x = 94$ har ordning 33 i $(U(\mathbb{Z}_{299}), \cdot)$. (Man kan också använda metoden i stencilen om kinesiska restsatsen.) (Alternativt: 2 har ordning $12 \cdot 11 = 132$ i U_{299} , så $2^4 = 16$ har ordning 33.)

Svar a: $\mathbb{Z}_{299}$ har 264 inverterbara element,

b: T.ex. 94 och 16 är element av ordning 33 i $(U(\mathbb{Z}_{299}), \cdot)$.